Information operations: part of full-spectrum battlefield

By Mike Schellhammer

The information age is changing how we view the world. The explosion of technology, the importance of automation, proliferation of global communications and the expansive nature of computer technology have changed military operations as they have the civilian world.

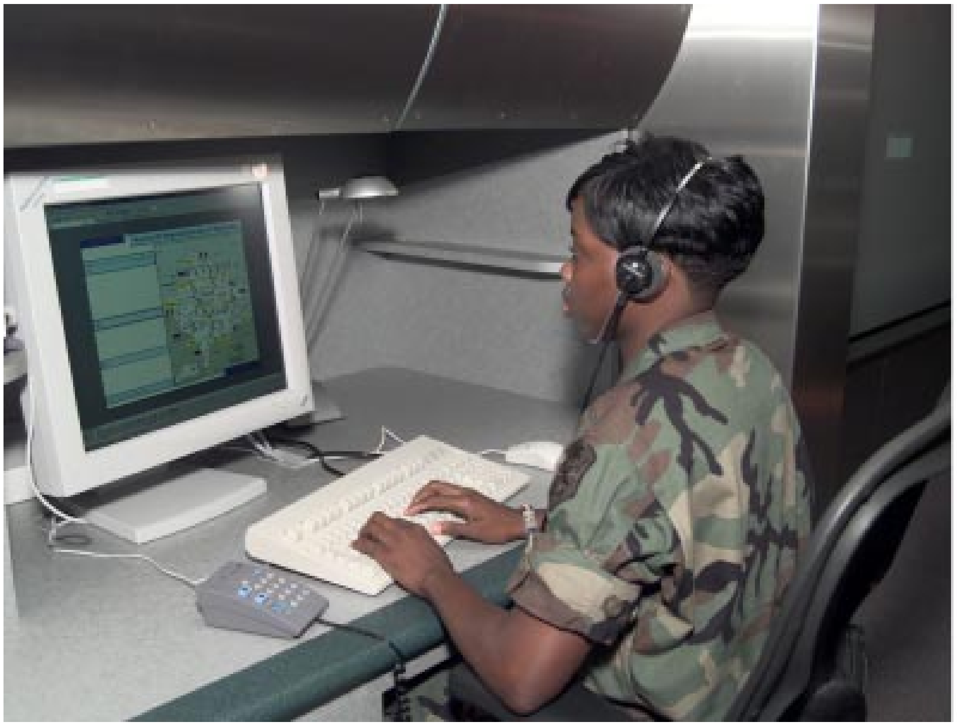
Rapid processing of battlefield and strategic information is vitally important to commanders at every level, and disruption of the flow of information can be as detrimental to an operation as physical destruction of personnel and equipment. The Army has recognized this course for several years, and now the doctrine for influencing an adversary's information flow while protecting our own is embodied in the concept of information superiority. As in any major Army effort, soldiers of the U.S. Army Intelligence and Security Command play an important role by providing intelligence support to information operations, one of the means used to achieve information superiority.

Although the term "information operations" usually evokes an image of computers and computer hackers, the term actually encompasses much more. FM 100-6, "Information Operations," defines IO as those actions taken to affect adversaries and influence other audiences' decision-making processes, information and information systems, while defending friendly information. Information operations can consist of separate actions by themselves or be a manner of focusing traditional military activity to define the operational situation, generate better understanding, provide context and influence perceptions. As explained by Jim Hoover, INSCOM deputy assistant G3 for information operations, "IO is a lot more than computers and hackers. It's how we manage and influence information in every operation."

"Full spectrum" information operations are as diverse as any conventional military activity. Offensive IO affects adversary decision-makers, processes and information management systems. For example, operational security (OPSEC), military deception and psychological operations are used to shape adversary perceptions, hide critical information or convey friendly themes. Electronic and computer network attacks are used to deny or degrade an adversary's capability to command and control his units. Physical destruction, using indirect or direct fire, is used to interdict or destroy information management systems.

Defensive IO protects our information and systems. It provides us with a more accurate, timely and comprehensive awareness of situations from many perspectives. For example, computer network defense and information assurance protect systems, detect intrusions, restore networks, deter further attacks and react to network probes. Counterintelligence, OPSEC, counterdeception, counterpropaganda and electronic warfare gather information and react to adversary collection efforts. With their inherent abilities to shape public opinion and perceptions, public affairs and civil affairs also can provide important support to offensive and defensive IO.

As with any operation, intelligence support is a vital component of IO, a fact well known to the INSCOM staff.



Military intelligence soldiers offer vital support for information operations. (Photo by Bob Bills)

In 1997, the command established the IO Division under the G3 to manage worldwide INSCOM intelligence support to IO. The division synchronizes IO efforts and includes intelligence collection, combat development for offensive IO, analysis and exploitation, counterintelligence support and military and technical production of IO-related products.

The Land Information Warfare Activity (LIWA) is the Army's operational focal point for all information operations and assists commanders worldwide with planning, preparing, executing and assessing IO. Some of the most visible LIWA support comes from its Field Support Teams (FSTs), the Army Computer Emergency Response Teams (ACERTs) and the IO Vulnerability Assessment Teams (IOVATs).

Operating from the LIWA headquarters at Fort Belvoir, Va., LIWA FSTs have deployed worldwide to provide direct IO support to land component and Joint Task Force (JTF) commanders. The FST often augment existing staffs and assist commanders in coordinating IO planning, intelligence and targeting. The teams usually consist of a field grade officer and three other military personnel with electronic warfare, operational security, military deception, civil affairs, public affairs, PSYOP, intelligence and computer network defense skills as required by the land component commander.

The ACERT has an around-the-clock coordination center at LIWA headquarters and provides capability to prevent, detect, assess and respond to Army information system security incidents in conjunction with four regional CERTs co-located at the Army Signal Command theater network and system operations centers at Fort Huachuca, Ariz.; Germany; Korea and Hawaii.

The IOVATs are designed to assess and enhance an Army commander's defensive IO capabilities. A holistic assessment employs a "Blue" team, which conducts non-intrusive assessments, and "Red" teams that simulate adversary IO capabilities and attacks. The teams provide commanders thorough, multidisciplined analysis of their vulnerabilities to IO attack and assist them in implementing defensive security measures.

Whereas the LIWA is the organizational focal point for the conduct of IO, the INSCOM Information Dominance Center (IDC) is the Army's IO tactical operations center. Located in INSCOM headquarters, the IDC will integrate and synchronize the Army's wide-ranging IO activities while supporting commanders with tailored analytical products, assessments, field support activities, computer emergency response and friendly vulnerability assessments. The IDC also will operate virtual and collaborative interfaces with other services, joint, national and U.S. government agencies. This ability to receive huge amounts of information and generate responses gives the IDC its nickname as the "brain stem" for intelligence support to IO.

Capable of 24-hour operations and manned by personnel from INSCOM headquarters, LIWA and other INSCOM units, the IDC will combine intelligence reports, open-source information and media sources into comprehensive IO-oriented databases. Analysts will then parse and search the data, looking for unique relationships and perspectives necessary to identify threat trends, and then continually refine the information to identify IO vulnerabilities and appropriate friendly courses of action. Commanders will be given a more complete "picture" of the IO battlefield than ever before.

Other INSCOM units also provide intelligence and offensive IO capabilities such as computer research, computer network exploitation and Special Purpose Electronic Attack. The 902nd Military Intelligence Group provides counterintelligence investigative support and computer media forensic analysis support to Army-wide IO. The National Ground Intelligence Center, which produces all-source intelligence estimates of adversary capabilities, also produces studies on potential adversary ground forces IO capabilities with threat projections based on exploitation of foreign material, modeling and simulation.

Despite the challenges presented by the information age, INSCOM will continue to play a significant role in enabling warfighters to achieve information superiority over adversaries. Harnessing the field and operational experiences of LIWA since 1995, the newly established IDC and the full range of INSCOM's worldwide multidisciplined intelligence, these capabilities are making INSCOM a recognized leader in ensuring full spectrum IO support to the Army is a reality.

Schellhammer is an intelligence specialist in the Measurement and Signature Intelligence Branch at INSCOM headquarters, Fort Belvoir, Va.

The Army Computer Emergency Response Team operates a coordination center 24 hours a day. (Photo by Bob Bills)